UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION

DENA BARRON, on behalf of herself, and all others similarly situated
22 John Street, 2b
Bloomfield, New Jersey 07003

Plaintiff,

v.

MARRIOTT INTERNATIONAL, INC.,
10400 Fernwood Road
Bethesda, Maryland 20817

Serve on: The Corporation Trust, Incorporated,
Resident Agent
2405 York Road, Suite 201
Lutherville, Maryland 21093-2264

Defendant.

Case No.

CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED

I. INTRODUCTION

Plaintiff, Dena Barron ("Plaintiff"), brings this action for herself and on behalf of all persons similarly situated ("Class Members") whose personally identifiable information ("PII") and other sensitive information was compromised by Marriott International, Inc. ("Marriott" or "Defendant") when the information of up to 500 million guests and consumers may have been accessed as part of a breach of its Starwood guest reservation database ("Starwood Data Breach").

II. JURISDICTION & VENUE

1. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and

costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendant and is a citizen of a foreign state. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

2. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant, as a corporate entity, does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions made by Marriott's governance and management personnel or inaction by those individuals that led to the Starwood Data Breach. Additionally, Marriott's terms of service governing users in the United States indicates that Maryland is the venue for all claims arising out of consumers' relationship with Marriott.

III. PARTIES

A. Plaintiff

3. Plaintiff Dena Barron is a citizen of the State of New Jersey.

4. In or about 2013, Plaintiff Barron joined the Marriott Starwood Rewards Program and obtained a Chase Marriott credit card.

5. Plaintiff Barron frequently stays at Marriott properties and hotels and generally earns or uses Starwood Rewards points on each visit.

6. When Plaintiff Barron joined the Marriott Starwood Rewards Program, she registered her personal credit card with Marriott.

7. In approximately September 2017, Plaintiff Barron received an alert that someone had fraudulently attempted to make a charge on her Chase Marriott credit card.

8. On or about November 30, 2018, Plaintiff Barron reviewed news accounts suggesting that her credit card account and other PII may have been compromised in the data

breach. In addition to the damages detailed herein, the Starwood Data Breach has caused Plaintiff Barron to be at substantial risk for further identity theft.

B. Defendant

9. Defendant, Marriott International, Inc., is and has been a Delaware corporation since approximately 1997. Marriott's corporate headquarters are located at 10400 Fernwood Road, Bethesda, Maryland. 20817.

IV. FACTUAL ALLEGATIONS

10. Marriott is an American multinational, diversified hospitality company that manages and franchises a broad portfolio of hotels and related lodging facilities, and is considered the largest hotel chain in the world, with more than 6,500 properties in 127 countries and territories globally, accommodating over 1.2 million rooms.

11. In 2017, Marriott produced a report of brand-wide revenue totaling more than $1.32 billion for the third fiscal quarter ending September 30, 2018.

12. Upon information and belief, Marriott collects, stores, and maintains information about its guests, including their PII, through its Starwood Guest Reservation Database ("Starwood Database").

13. Upon information and belief, on or about September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood Database.

14. Upon information and belief, Marriott has determined that the Starwood Database had been accessed by unauthorized users since 2014, including through copying and encrypting information about Plaintiff and Class members.

15. On or about November 19, 2018, Marriott determined that the contents of the copied and encrypted information were from the Starwood Database.

16. Marriott has reported publicly that the Starwood Database contains information on up to approximately 500 million guests who made a reservation at a Starwood property, and that for approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.

17. Additionally, Marriott has reported that for some of its guests, the information retrieved from the Starwood Database also includes payment card numbers and payment card expiration dates.

18. The Starwood Data Breach poses potential and actual problems for consumers, including the ability of a perpetrator to gain access to different areas of a victim's digital life (such as bank accounts, social media, and credit card details) and to harvest other sensitive data, as well as information belonging to family, friends, and colleagues.

19. At all times relevant hereto, Marriott knew or should have known of its obligation to protect the personal and financial data of its guests and customers because of its participation in the storage of PII and other sensitive information (including but not limited to storage of payment card information), as well as interactions with payment card processing networks. Marriott was also aware of the significant repercussions if it failed to do so because Marriott collected payment card data from hundreds of millions of guests and customers daily and it knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

20. Despite understanding the consequences of inadequate data security, Marriott failed to take appropriate protective measures to protect and secure guests' and customers' PII and other sensitive information, including data belonging to Plaintiff and Class members.

21. Despite understanding the consequences of inadequate data security, Marriott operated computer network systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; failed to detect intrusions dating back as far as 2014; and, failed to take other measures necessary to protect its data network.

V. CLASS ALLEGATIONS

22. Plaintiff brings this lawsuit as a class action on behalf of themselves and all other Class Members similarly situated pursuant to Federal Rules of Civil Procedure 23(a) and (b)(2), (b)(3), and/or (c)(4). This action satisfies the numerosity, typicality, adequacy of representation, predominance of common issues, and superiority requirements of those provisions

23. As alleged throughout this Complaint, Plaintiff's and the Class' claims all derive directly from a single course of conduct by Marriott. This case is about the responsibility of Marriott, at law and in equity, for its knowledge, its conduct, and its actions. Marriott has engaged in uniform and standardized conduct toward Plaintiff and the Class. It did not differentiate, in its degree of care or candor, its actions or inactions, or in the content of its statements or omissions, among individual Class members. The objective facts on these subjects are the same for all Class members. Within each cause of action asserted by the respective Classes, the same legal standards govern.

24. Pursuant to Rules 23(a); (b)(2); and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff brings this action and seek to certify and maintain it as a class action on

behalf of themselves and a Nationwide Class, as defined below, or, in the alternative, for statewide State Classes, as defined below.

25. Plaintiff seeks a Nationwide Class (or State Classes) for damages under Rule 23(b)(3) for those Class Members who have experienced the theft of PII and other sensitive information as a result of the Starwood Data Breach.

26. Plaintiff seeks a Nationwide Class (or State Classes) for declaratory relief under Rule 23(b)(2) for those individuals who have not yet experienced the effect of the Starwood Data Breach.

A. The Nationwide Class

27. The Nationwide Class is initially defined as follows:

> All persons in the United States who provided PII and/or other sensitive information (including but not limited to credit card information) to Marriott (or its subsidiaries) and whose PII was accessed, compromised, and/or stolen from Marriott in the Starwood Data Breach.

B. The State Classes

28. In the alternative to the Nationwide Class, Plaintiff alleges statewide class action claims on behalf of state-wide classes for certain states ("State Classes"). Each of these State Classes is initially defined as follows:

Maryland Class

> All residents of Maryland who provided PII and/or other sensitive information (including but not limited to credit card information) to Marriott (or its subsidiaries) and whose PII was accessed, compromised, and/or stolen from Marriott in the Starwood Data Breach.

New Jersey Class

> All residents of New Jersey who provided PII and/or other sensitive information (including but not limited to credit card information) to Marriott (or its subsidiaries) and whose PII was accessed, compromised, and/or stolen from Marriott in the Starwood Data Breach.

29. The Nationwide Class and the State Classes and their members are sometimes referred to herein as the "Class" or "Classes."

30. Excluded from the proposed Class are: (1) Marriott, any entity or division in which Marriott has a controlling interest, and its legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's immediate family and staff; (3) governmental entities; and (4) those persons who have suffered personal injuries as a result of the facts alleged herein. Plaintiff reserves the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, otherwise divided into subclasses, or modified in any other way.

Numerosity

31. Although the exact number of Class Members is uncertain and can only be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable. The disposition of the claims of these Class Members in a single action will provide substantial benefits to all parties and to the Court. Class Members are readily identifiable from information and records in Marriott's possession, custody, or control.

Typicality

32. The claims of Plaintiff are typical of the claims of Class Members in that Plaintiff, like all Class Members, provided PII (including but not limited to credit card information) and other sensitive information to Marriott (or its subsidiaries) which PII and other sensitive information was accessed, compromised, and/or stolen from Marriott in the Starwood Data Breach.

33. Furthermore, the factual bases of Marriott's misconduct are common to all Class Members and represent a common thread of misconduct resulting in injury to all Class Members.

Adequate Representation

34. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff has retained counsel with substantial experience in prosecuting consumer class actions.

35. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of Class Members, and have the financial resources to do so. Neither Plaintiff nor her counsel have interests adverse to those of Class Members.

Predominance of Common Issues

36. There are numerous questions of law and fact common to Plaintiff and Class Members that predominate over any question affecting only individual Class Members, the answers to which will advance resolution of the litigation as to all Class Members. These common legal and factual issues include:

a. Whether Class members' PII was accessed, compromised, or stolen in the Starwood Data Breach;

b. Whether (and when) Defendant knew about any security vulnerabilities that led to the Starwood Data Breach before it was announced to the public and whether Defendant failed to timely notify the public of those vulnerabilities and the Starwood Data Breach;

c. Whether Defendant's representations that it would secure and protect the PII and other sensitive information of Plaintiff and Class members were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendant's services;

d. Whether such representations were false with regard to storing and safeguarding Plaintiff and Class members' PII and other sensitive information;

e. Whether Defendant misrepresented the safety and security of its many systems and services, and its ability to safely store Plaintiff and Class members' PII and other sensitive information;

f. Whether such representations were material with regard to storing and safeguarding Class members' PII.

g. Whether Defendant concealed crucial information about its inadequate data security measures from Plaintiff and the Class;

h. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class members' PII and other sensitive information secure and prevent the loss or misuse of that information;

i. Whether Defendant owed a duty to Plaintiff and the Class to safeguard their PII and to implement adequate data security measures;

j. Whether Defendant breached that duty;

k. Whether Defendant failed to "implement and maintain reasonable security procedures and practices" for Plaintiff's and Class members' PII in violation of Section 5 of the FTCA;

l. Whether Defendant violated the Maryland Consumer Protection Act, Md. Code Com. Law §§ 14-3501, et seq., by failing to inform consumers (including Plaintiff and the Class Members) of its unsecure, uncompliant, and otherwise insufficient data and information security practices;

m. Whether Defendant violated the Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3504(b), by failing to promptly investigate the

Starwood Data Breach and/or to notify Plaintiff and Class Members of the Starwood Data Breach's existence; and

37. Whether Defendant violated the New Jersey Consumer Fraud Act, N.J. STAT. ANN. §§ 56:8-1, et seq., by failing to inform consumers (including Plaintiff and the Class Members) of its unsecure, uncompliant, and otherwise insufficient data and information security practices.

Superiority

38. Plaintiff and Class Members have all suffered and will continue to suffer harm and damages as a result of Marriott's unlawful and wrongful conduct. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

39. Absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Because of the relatively small size of the individual Class Members' claims (compared to the cost of litigation), it is likely that only a few Class Members could afford to seek legal redress for Marriott's misconduct. Absent a class action, Class Members will continue to incur damages, and Marriott's misconduct will continue without remedy.

40. Class treatment of common questions of law and fact would also be a superior method to multiple individual actions or piecemeal litigation in that class treatment will conserve the resources of the courts and the litigants, and will promote consistency and efficiency of adjudication.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE

[Applicable to Nationwide Class and/or Maryland and/or New Jersey Class(es)]

41. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

42. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII and other sensitive information, and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the PII and other sensitive information of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

43. By being entrusted by Plaintiff and the Class to safeguard their PII and other sensitive information, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class signed up for and paid for Defendant's services and agreed to provide their PII and other sensitive information with the understanding that Defendant would take appropriate measures to protect it, and would inform Plaintiff and the Class of any breaches or other security concerns that might call for action by Plaintiff and the Class.

44. Defendant failed to take appropriate measures to protect the PII and other sensitive information of Plaintiff and the Class. Defendant is morally culpable, given the prominence of security breaches in the hospitality industry, and especially given the admission that this data vulnerability dates back to 2014, demonstrating Defendant's wholly inadequate safeguards, and refusal to notify Plaintiff and the Class of breaches or security vulnerabilities.

45. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII and other sensitive information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite repeated failures and intrusions, and allowing unauthorized access to Plaintiff's and the other Class member's PII and other sensitive information.

46. Defendant's failure to comply with industry and federal regulations further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII and other sensitive information.

47. Defendant's breaches of these duties were not merely isolated incidents or small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term companywide refusal by Defendant to acknowledge and correct serious and ongoing data security problems again, as evidenced by this vulnerability existing since 2014.

48. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII and other sensitive information would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII and other sensitive information of Plaintiff and the Class and all resulting damages.

49. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII and other sensitive information. Defendant knew its systems and technologies for processing and securing the PII and other sensitive information of Plaintiff and the Class had numerous security vulnerabilities.

50. As a result of this misconduct by Defendant, the PII and other sensitive information of Plaintiff and the Class was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII and other sensitive information was disclosed to third parties without their consent. Plaintiff and the Class have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

51. Defendant's misconduct as alleged herein is malice or oppression, in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff and the Class and despicable conduct that has subjected Plaintiff and the Class to cruel and unjust hardship in conscious disregard of their rights.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE

[Applicable to Nationwide Class and/or Maryland and/or New Jersey Class(es)]

52. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

53. Section 5 of the Federal Claims Tort Act ("FTCA"), 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Marriott, of failing to use reasonable measures to protect PII.

54. Marriott violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Marriott's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored (approximately 500 million unique guests and consumers), and the foreseeable

consequences of a data breach at a hospitality chain as large as Marriott, including, specifically, the immense damages that would result to Plaintiff and Class members.

55. Marriott's violation of Section 5 of the FTCA constitutes negligence per se.

56. Plaintiff and Class members are within the class of persons that the FTCA was intended to protect.

57. The harm that occurred as a result of the Starwood Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

58. As a direct and proximate result of Marriott's negligence per se, Plaintiff and the Class have suffered, continue to suffer, and anticipate suffering, injuries and damages arising from identity theft; Plaintiff and Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Starwood Data Breach and/or false or fraudulent charges stemming from the Starwood Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Starwood Data Breach on their lives, including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

59. Additionally, as a direct and proximate result of Marriot's negligence per se, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Marriott's possession and is subject to further unauthorized disclosures so long as Marriott fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

THIRD CAUSE OF ACTION
VIOLATION OF MARYLAND'S CONSUMER PROTECTION ACT, MARYLAND CODE ANN., COMM. LAW §§ 13-101 et seq.

[Applicable to Maryland Class]

60. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

61. The Maryland Consumer Protection Act ("MCPA"), prohibits "persons" from engaging in "any unfair or deceptive trade practice," including for "consumer services." Md. Code Ann., Com. Law § 13-303.

62. Marriott is a "merchant" and "person" for the purposes of the MCPA, Md. Code Ann., Com. Law § 13-101(g) and (h), respectively, and was, at all times relevant herein, engaged in soliciting "consumer services" as that term is defined at the MCPA, Md. Code Ann., Com. Law § 13-101(d), by soliciting an ongoing service, credit reporting and data aggregation of Plaintiff's personal information, to consumers in Maryland for primarily personal use within the meanings specified in the MCPA.

63. Plaintiff and Class members are "consumers" for purposes of the MCPA, Md. Code Ann., Com. Law § 13-101(c).

64. Defendant, by failing to inform consumers (including Plaintiff and Class members) of its unsecure, uncompliant, and otherwise insufficient data and information security

practices, advertised, sold, serviced, and otherwise induced those consumers (including Plaintiff and Class members) to purchase goods and services from Defendant.

65. By failing to inform consumers (including Plaintiff and the Class members) of its unsecure, uncompliant, and otherwise insufficient data and information security practices, Defendant falsely represented the security of its data and information security practices to safeguard the PII and other sensitive information that Defendant collected on consumers (including Plaintiff and Class members).

66. Defendant is therefore in violation of the MCPA.

FOURTH CAUSE OF ACTION
VIOLATION OF MARYLAND'S PERSONAL INFORMATION PROTECTION ACT, MARYLAND CODE ANN., COMM. LAW §§ 14-3501 et seq.

[Applicable to Maryland Class]

67. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

68. The Maryland Personal Information Protection Act ("MPIPA") requires businesses that own or license computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, to promptly investigate the likelihood that personal information has been or will be misused as a result of the breach, and to then notify affected individuals of the breach. Md. Code Ann., Com. Law § 14-3504(b).

69. Upon information and belief, Defendant identified the Starwood Data Breach as early as September 2018, but only identified consumers on November 30, 2018, thus placing those consumers at risk for the months in between the discovery and notification of the Starwood Data Breach.

70. Defendant's failures constitute false, misleading, and misrepresentations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class members) concerning the security of their networks and aggregation of PII.

71. In addition, the facts upon which consumers (including Plaintiff and Class members) relied were material facts which was un true (e.g., protection of PII), and consumers (including Plaintiff and Class members) relied on those false facts to their detriment.

72. Defendant employed these false representations to promote the sale of a consumer good or service, which Plaintiff and the Class members purchased.

73. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

74. Through failing to promptly investigate the Starwood Data Breach and/or to notify Plaintiff and Class members of the Starwood Data Breach's existence, Defendant is in violation of the MPIPA.

FIFTH CAUSE OF ACTION
VIOLATION OF NEW JERSEY'S
CONSUMER FRAUD ACT, §§ 56:8-1 et seq.

[Applicable to New Jersey Class]

75. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

76. The New Jersey Consumer Fraud Act, N.J. STAT. ANN. §§ 56:8-1, et seq. ("NJCFA") protects consumers against "any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment,

suppression or omission, in connection with the sale or advertisement of any merchandise…" N.J. STAT. ANN. §56:8-2.

77. Defendant, by failing to inform consumers (including Plaintiff and Class members) of its unsecure, uncompliant, and otherwise insufficient data and information security practices, advertised, sold, serviced, and otherwise induced those consumers (including Plaintiff and Class members) to purchase goods and services from Defendant.

78. By failing to inform consumers (including Plaintiff and Class members) of its unsecure, uncompliant, and otherwise insufficient data and information security practices, Defendant falsely represented the security of its data and information security practices to safeguard the PII and other sensitive information that Defendant collected on consumers (including Plaintiff and Class members).

79. Plaintiff and other Class members' damages are the direct and foreseeable result of Defendant's unlawful conduct.

80. Therefore, Defendant has violated the New Jersey Consumer Fraud Act.

RELIEF REQUESTED

WHEREFORE, Plaintiff, on behalf of herself, and all others similarly situated, request the Court to enter judgment against Marriott, as follows:

a. an order certifying the proposed Class and/or any appropriate subclasses, designating Plaintiff as named representative of the Class, and designating the undersigned as Class Counsel;

b. a declaration that: Class members' PII was accessed, compromised, or stolen in the Starwood Data Breach; Defendant knew about security vulnerabilities that led to the Starwood Data Breach before it was announced to the public; Defendant's representations that it would secure and protect the PII and other sensitive information of Plaintiff and Class members

were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendant's services; such representations were false with regard to storing and safeguarding Plaintiff and Class members' PII and other sensitive information; and that Defendant misrepresented the safety and security of its many systems and services, and its ability to safely store Plaintiff and Class members' PII and other sensitive information;

c. a declaration that Defendant owed a duty to Plaintiff and the Class to safeguard their PII and to implement adequate data security measures;

d. a declaration that Defendant breached that duty;

e. a declaration that Defendant has failed to "implement and maintain reasonable security procedures and practices" for Plaintiff and Class members' PII in violation of Section 5 of the FTCA;

f. a declaration that Defendant has, through its conduct, violated the Maryland Consumer Protection Act, Md. Code Com. Law §§ 14-3501, et seq.,; the Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3504(b); and the New Jersey Consumer Fraud Act, N.J. STAT. ANN. §§ 56:8-1, et seq.;

g. an order enjoining Marriott from further deceptive practices;

h. an award to Plaintiff and Class members of compensatory, exemplary, and statutory damages, including interest, in an amount to be proven at trial;

i. an award of attorneys' fees and costs as allowed by law;

j. an award of pre-judgment and post-judgment interest, as provided by law;

k. leave to amend this Complaint to conform to the evidence produced at trial; and

l. such other relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Dated: December 3, 2018

Respectfully submitted,

/s/ James P. Ulwick
James P. Ulwick (Bar No. 00536)
KRAMON & GRAHAM, P.A.
One South Street, Suite 2600
Baltimore, Maryland 21202
(410) 752-6030
(410) 539-1269 (facsimile)
julwick@kg-law.com

Joseph G. Sauder
Matthew D. Schelkopf
Joseph B. Kenney
SAUDER SCHELKOPF, LLC
555 Lancaster Avenue
Berwyn, Pennsylvania 19312
(610) 200-0580
(610)727-4360 (facsimile)
jgs@sstriallawyers.com
mds@sstriallawyers.com
jbk@sstriallawyers.com

Counsel for Plaintiff and the Putative Class